Electronic Version
Stylesheet Version v1.1.1

Description

SYSTEM AND METHOD FOR SECURING RF TRANSACTIONS USING A RADIO FREQUENCY IDENTIFICATION DEVICE INCLUDING A TRANSACTIONS COUNTER

Cross Reference to Related Applications

[0001] This invention is a continuation in part of, and claims priority to U.S. Patent Application No. 10/192,488, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed on July 9, 2002 (which itself claims priority to U.S. Provisional Patent Application No. 60/304,216, filed July 10, 2001), and to U.S. Patent Application No. 10/340,352, entitled "SYSTEM AND METHOD FOR INCENTING PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed January 10, 2003 (which itself claims priority to U.S. Provisional Patent Application No.

60/396,577, filed July 16, 2002), all of which are incorporated herein by reference.

FIELD OF INVENTION

[0002] This invention generally relates to a system and method for securing a Radio Frequency (RF) transaction using a RF operable device, and more particularly, to securing a RF transaction using a Radio Frequency Identification (RFID) device including a random number sequencer.

BACKGROUND OF INVENTION

[0003] Like barcode and voice data entry, RFID is a contactless information acquisition technology. RFID systems are wireless, and are usually extremely effective in hostile environments where conventional acquisition methods fail. RFID has established itself in a wide range of markets, such as, for example, the high-speed reading of railway containers, tracking moving objects such as livestock or automobiles, and retail inventory applications. As such, RFID technology has become a primary focus in automated data collection, identification and analysis systems worldwide.

[0004] Of late, companies are increasingly embodying RFID data acquisition technology in a fob or tag for use in complet-

ing financial transactions. A typical fob includes a transponder and is ordinarily a self-contained device which may be contained on any portable form factor. In some instances, a battery may be included with the fob to power the transponder, in which case the internal circuitry of the fob (including the transponder) may draw its operating power from the battery power source. Alternatively, the fob may exist independent of an internal power source. In this instance the internal circuitry of the fob (including the transponder) may gain its operating power directly from an RF interrogation signal. U.S. Patent No. 5,053,774, issued to Schuermann, describes a typical transponder RF interrogation system which may be found in the prior art. The Schuermann patent describes in general the powering technology surrounding conventional transponder structures. U.S. Patent No. 4,739,328 discusses a method by which a conventional transponder may respond to a RF interrogation signal. Other typical modulation techniques which may be used include, for example, ISO/IEC 14443 and the like.

[0005] In the conventional fob powering technologies used, the fob is typically activated upon presenting the fob in an interrogation signal. In this regard, the fob may be activated

irrespective of whether the user desires such activation. Alternatively, the fob may have an internal power source such that interrogation by the reader to activate the fob is not required.

[0006] One of the more visible uses of the RFID technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products. These products use transponders placed in a fob or tag which enables automatic identification of the user when the fob is presented at a Point of Sale (POS 106) device. Fob identification data is typically passed to a third-party server database, where the identification data is referenced to a customer (e.g., user) credit or debit account. In an exemplary processing method, the server seeks authorization for the transaction by passing the transaction and account data to an authorizing entity, such as for example an "acquirer" or account issuer. Once the server receives authorization from the authorizing entity, the authorizing entity sends clearance to the point of sale device for completion of the transaction.

[0007] Minimizing fraud transactions in the RFID environment is typically important to the account issuer to lessen the loss associated with fraudulent RFID transaction device usage.

One conventional method for securing RFID transactions involves requiring the device user to provide a secondary form of identification during transaction completion. For example, the RFID transaction device user may be asked to enter a personal identification number (PIN) into a key-pad. The PIN may then be verified against a number associated with the user or the RFID transaction device, where the associated number is stored in an account issuer database. If the PIN number provided by the device user matches the associated number, then the transaction may be cleared for completion.

[0008] One problem with the conventional method of securing an RFID transaction is that the time for completing the transaction is increased. This is true since the RFID device user must delay the transaction to provide the alternate identification. As can be seen, this defeats one real advantage of the RFID transaction device, which is to permit expedient completion of a transaction.

[0009] As such, a need exists for a method of securing RFID transaction which does not increase the time needed to complete a transaction, and which method may be used without device user intervention.

SUMMARY OF INVENTION

[0010] Described herein is a system and method for securing RFID transactions which addresses the problems found in conventional transaction securing methods. The securing method described herein includes providing a randomly generated indicia for use in determining whether a device is authorized to complete a transaction request over a system including radio frequency transmission. As such, the invention provides a radio frequency operable transaction device including a transaction device random number generator which may generate a random number in response to a transaction request or RFID reader provided interrogation signal. The transaction device random number may be provided to a transaction device issuer for use in determining whether the transaction device providing transaction account information is an authorized device for use in completing a transaction on the system of the invention. The account issuer may use the random number to locate the appropriate verifying (e.g., "validating") information for confirming the transaction device validity.

[0011] During operation, the RFID transaction device may be interrogated by a RFID reader operable to provide a RF interrogation signal for powering a transponder system. The RFID reader may receive an encrypted RFID transaction

device identifier, and the transaction device random number from the RFID transaction device and provide the identifier and random number to an authorizing entity, such as an acquirer or an account issuer, for verification. Once the authorizing agent verifies the validity of the transaction device identifier using the random number, the authorizing entity (e.g., account issuer or acquirer) may provide clearance that a transaction may be completed.

[0012] In one exemplary embodiment, the RFID transaction device may include an authentication tag which may be provided to the RFID reader along with the random number and the transaction account identifier. The RFID reader may then provide the random number transaction device identifier and authentication tag to the authorizing agent for verification. Once validated, the authorizing agent may provide indication to the merchant point of sale terminal that the transaction may be completed.

[0013] In another exemplary embodiment, the RFID reader may additionally be "validated" as being authorized to facilitate transactions with the account issuer. In this instance, the RFID reader may be equipped with a RFID reader authentication tag and a random number generator for generating

a RFID reader random number. In this way, once the RFID reader receives the RFID transaction device identifier, the RFID reader may provide the transaction device identifier, RFID reader random number, and reader authentication tag to an authorizing agent, such as an acquirer. The acquirer may then validate that the RFID reader is an authorized reader for facilitating a RF transaction with the account issuer. If the RFID reader authentication tag is validated, the acquirer may then provide the RFID transaction device identifier to an account provider for RFID device verification. The account issuer may then verify that the RFID transaction device is authorized to complete the requested transaction.

[0014] In yet another embodiment of the invention, both the RFID reader and the RFID transaction device include an authentication tag. In this embodiment, the RFID transaction device authentication tag and the RFID reader authentication tag may be verified by the account issuer using a transaction device random number and a reader random number, respectively. In this instance the authorizing entity may validate both the transaction device and the reader prior to permitting the requested transaction to be completed.

[0015] In still another embodiment of the present invention, the

reader authentication tag, the transaction device authentication tag, and the RFID device identifier may be encrypted. In this embodiment, either the RFID transaction device, the RFID reader, or both, include a random number generator for generating a random number to be used to validate the RFID transaction device or the RFID reader. The account issuer may receive the device and reader authentication tags and the device and reader random numbers and use the random numbers to locate the proper decryption keys for decrypting the authentication tags, or encrypted identifiers for validation. Once the information is validated, the account issuer may provide clearance to a merchant system for transaction completion.

[0016] These features and other advantages of the system and method, as well as the structure and operation of various exemplary embodiments of the system and method, are described below.

Brief Description of Drawings

[0017] The accompanying drawings, wherein like numerals depict like elements, illustrate exemplary embodiments of the present invention, and together with the description, serve to explain the principles of the invention. In the drawings:

[0018] FIG 1 illustrates an exemplary RFID-based system depict-

ing exemplary components for use in RFID transaction completion in accordance with the present invention;

[0019] FIG 2 illustrates an exemplary method for securing a RFID transaction by validating a RFID transaction device using a random number in accordance with the present invention;

[0020] FIG 3 illustrates an exemplary RF transaction security method for validating a RFID reader using a random number and RFID transaction device authentication tag in accordance with the present invention; and

[0021] FIG 4 illustrates an exemplary RF transaction security method for validating a RFID transaction device using a transaction device random number and RFID for validating a RFID reader using a reader transaction device in accordance with the present invention.

DETAILED DESCRIPTION

[0022] The present invention may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. Such functional blocks may be realized by any number of hardware and/or software components configured to perform to specified functions. For example, the present invention may employ various integrated circuit components ((e.g., memory elements, processing elements, logic elements, look-up ta-

bles, and the like), which may carry out a variety of functions under the control of one or more mircroprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, extensible markup language (XML), JavaCard and MULTOS with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction on cryptography, review a text written by Bruce Schneier entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons (second edition, 1996), herein incorporated by reference.

[0023] In addition, many applications of the present invention could be formulated. The exemplary network disclosed herein may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. It is noted that the network may be implemented as

other types of networks, such as an interactive television network (ITN).

[0024] Further still, the terms "Internet" or "network" may refer to the Internet, any replacement, competitor or successor to the Internet, or any public or private inter-network, intranet or extranet that is based upon open or proprietary protocols. Specific information related to the protocols, standards, and application software utilized in connection with the Internet may not be discussed herein. For further information regarding such details, see, for example, Dilip Naik, "Internet Standards and Protocols" (1998); "Java 2 Complete," various authors, (Sybex 1999); Deborah Ray and Eric Ray, "Mastering HTML 4.0" (1997); Loshin, "TCP/IP Clearly Explained" (1997). All of these texts are hereby incorporated by reference.

[0025] By communicating, a signal may travel to/from one component to another. The components may be directly connected to each other or may be connected through one or more other devices or components. The various coupling components for the devices can include but are not limited to the Internet, a wireless network, a conventional wire cable, an optical cable or connection through air, water, or any other medium that conducts signals, and any

other coupling device or medium.

[0026] Where required, the system user may interact with the system via any input device such as, a keypad, keyboard, mouse, kiosk, personal digital assistant, handheld computer (e.g., Palm Pilot®, Blueberry®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, work station, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris, or the like. Moreover, although the invention may frequently be described as being implemented with TCP/IP communications protocol, it should be understood that the invention could also be implemented using SNA, IPX, Appletalk, IPte, NetBIOS, OSI or any number of communications protocols. Moreover, the system contemplates, the use, sale, or distribution of any goods, services or information over any network having similar functionality described herein.

[0027] A variety of conventional communications media and protocols may be used for data links providing physical connections between the various system components. For example, the data links may be an Internet Service Provider

(ISP) configured to facilitate communications over a local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Lines (DSL), or any wireless communication media. In addition, the merchant system including the POS 106 device 106 and host network 108 may reside on a local area network which interfaces to a remote network (not shown) for remote authorization of an intended transaction. The POS 106 106 may communicate with the remote network via a leased line, such as a T1, D3 line, or the like. Such communications lines are described in a variety of texts, such as, "Understanding Data Communications," by Gilbert Held, which is incorporated herein by reference.

[0028] A transaction device identifier, as used herein, may include any identifier for a transaction device which may be correlated to a user transaction account (e.g., credit, charge debit, checking, savings, reward, loyalty, or the like) maintained by a transaction account provider (e.g., payment authorization center). A typical transaction account identifier (e.g., account number) distinct to a transaction device, may be correlated to a credit or debit account, loyalty account, or rewards account maintained and

serviced by such entities as American Express, Visa and/or MasterCard or the like.

[0029] A transaction device identifier may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000." In a typical example, the first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and, etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer. The account number may be stored as Track 1 and Track 2 data as defined in ISO/IEC 7813, and further may be made unique to the RFID transaction device.

[0030] In one exemplary embodiment, the transaction device identifier may include a unique RFID transaction device serial number and user identification number, as well as specific application applets. The transaction device identi-

fier may be stored on a transaction device database located on the transaction device. The transaction device database may be configured to store multiple account numbers issued to the RFID transaction device user by the same or different account providing institutions. In addition, where the device identifier corresponds to a loyalty or rewards account, the RFID transaction device database may be configured to store the attendant loyalty or rewards points data.

[0031] In addition to the above, the transaction device identifier may be associated with any secondary form of identification configured to allow the consumer to interact or communicate with a payment system. For example, the transaction device identifier may be associated with, for example, an authorization/access code, personal identification number (PIN), Internet code, digital certificate, biometric data, and/or other secondary identification data used to verify a transaction device user identity.

[0032] An authentication tag, as used herein, is any indicia which may be provided for use as a secondary identifier for a device. The authentication tag may be used with or without a transaction card identifier, but is preferably used along with the identifier. The authentication tag may be

specific to a particular account provider, such that, multiple devices (e.g., transaction devices, reader, etc.) may contain the same authentication tag.

[0033] To facilitate understanding, the present invention may be described with respect to a credit account. However, it should be noted that the invention is not so limited and other accounts permitting an exchange of goods and services for an account data value is contemplated to be within the scope of the present invention.

[0034] The databases discussed herein may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Common database products that may be used to implement the databases include DB2 by IBM (White Plains, New York), any of the database products available from Oracle Corporation (Redwood Shores, California), Microsoft Access or MSSQL by Microsoft Corporation (Redmond, Washington), or any other database product. Databases may be organized in any suitable manner, including as data tables or lookup tables. Association of certain data may be accomplished through any data association technique known and practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques

may include, for example, a database search, a database merge, GREP, AGREP, SQL, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in each of the manufacturer and retailer data tables. A "key field" partitions the database according to the high-level class of objects defined by the key field. For example, a certain class may be designated as a key field in both the first data table and the second data table, and the two data tables may then be merged on the basis of the class data in the key field. In this embodiment, the data corresponding to the key field in each of the merged data tables is preferably the same. However, data tables having similar, though not identical, data in the key fields may also be merged by using AGREP, for example.

[0035] It should be further noted that conventional components of RFID transaction devices may not be discussed herein for brevity. For example, one skilled in the art will appreciate that the RFID transaction device and the RFID reader disclosed herein include traditional transponders, antennas, protocol sequence controllers, modulators/demodulators and the like, necessary for proper RFID data transmission. As such, those components are contem-

plated to be included in the scope of the invention.

[0036] Further still, various components may be described herein in terms of their "validity." In this context, a "valid" component is one which is authorized for use in completing a transaction request in accordance with the present invention. Contrarily, an "invalid" component is one which is not authorized for transaction completion. In addition, an invalid component may be one which is not recognized as being permitted for use on the secure RF system described herein.

[0037] Although the present invention is described with respect to validating a transaction device or reader communicating in a RF transaction, the invention is not so limited. The invention, including the random number validation process described herein, may be used for any device, machine, or article, which may be used to transmit RF-based information over a secure RF network.

[0038] Figure 1 illustrates an exemplary secure RFID transaction system 100 in accordance with the present invention, wherein exemplary components for use in completing a RF transaction are depicted. In general, system 100 may include a RFID transaction device 102 in RF communication with a RFID reader 104 for transmitting data there

between. The RFID reader 104 may be in further communication with a merchant point of sale (POS) device 106 for providing to the POS 106 data received from the RFID transaction device 102. The POS 106 may be in further communication with an acquirer 110 or an account issuer 112 via a network 108 for transmitting transaction request data and receiving authorization concerning transaction completion.

[0039] Although the point of interaction device is described herein with respect to a merchant point of sale device 106, the invention is not to be so limited. Indeed, a merchant POS device is used herein by way of example, and the point of interaction device may be any device capable of receiving transaction device account data. In this regard, the POS 106 may be any point of interaction device enabling the user to complete a transaction using a transaction device 102. The POS device 106 may receive RFID transaction device 102 information and provide the information to host network 108 for processing.

[0040] As used herein, an "acquirer" may be a third-party entity including various databases and processors for facilitating the routing of a payment request to an appropriate account issuer 112. The acquirer 110 may route the pay-

ment request to the account issuer 112 in accordance with a routing number provided by the RFID transaction device 102, where the routing number corresponds to the account issuer 112. The "routing number" in this context may be a unique network address or any similar device for locating an account issuer 112 on a network 108. In one exemplary embodiment, the routing number may typically be stored in magnetic stripe 100 format on one of the tracks comprising the magstripe network. Traditional means of routing payment request in accordance with the routing number are well understood. As such, the process for using routing number to provide payment request will not be discussed herein for brevity.

[0041] In addition, the account issuer 112 ("account provider") may be any entity which provides a transaction account useful for facilitating completion of a transaction request. The transaction account may be identified by an account identifier or account number as described above. The transaction account may be any credit, debit, loyalty, direct debit, checking, or savings, or the like. The term "issuer" or "account provider" may refer to any entity facilitating payment of a transaction using a transaction device, and which may include systems permitting payment using

at least one of a preloaded and non-preloaded transaction device 102. Typical issuers may be American Express, MasterCard, Visa, Discover, and the like. In the preloaded value processing context, an exchange value (e.g., money, rewards points, barter points, etc.) may be stored in a preloaded value database (not shown) for use in completing a requested transaction. The preloaded value database and thus the exchange value may not be stored on the transaction device 102 itself, but may be stored remotely, such as for example at the account issuer 112 location. Further, the preloaded value database may be debited the amount of the transaction requiring the value to be replenished. The preloaded value may be any conventional value (e.g., monetary, rewards points, barter points, etc.) which may be exchanged for goods or services. In that regard, the preloaded value may have any configuration as determined by the issuer system 112.

[0042] In general, during operation of secure system 100, the RFID reader 104 may provide an interrogation signal to transaction device 102 for powering the device 102 and receiving transaction device related data. The interrogation signal may be received at the transaction device antenna 120 and may be further provided to a transponder

(not shown). In response, the transaction device processor 114 may retrieve a transaction device identifier and transaction device authentication code from transaction device database 116 for providing to the RFID reader to complete a transaction request. Typically, the transaction device identifier or the transaction device authentication tag may be encrypted prior to providing the device identifier to a modulator/demodulator (not shown) for providing the identifier and tag to the RFID reader 104.

[0043] It should be noted that the RFID reader 104 and the RFID transaction device 102 may engage in mutual authentication prior to transferring any transaction device 102 data to the reader 104. For a detailed explanation of a suitable mutual authentication process for use with the invention, please refer to commonly owned U.S. Patent Application No. 10/340,352, entitled "System and Method for Incenting Payment Using Radio Frequency Identification in Contact and Contactless Transactions," filed January 10, 2003, incorporated by reference in its entirety.

[0044] In accordance with the present invention, a RF transaction is secured by evaluating the validity of a RFID transaction device 102 using a random number. As described more fully below, an account authorizing agent, such as an ac-

count issuer 112 may receive the random number and use the number to locate validating information stored on the account issuer 112 system. The validating information may be any data stored on the account issuer 112 system which may be used to verify that the transaction device and/or the information provided by the transaction device ("transaction device information") are authorized elements which correspond to an authorized transaction account for completing a transaction request.

[0045] This method of securing RF transactions using a RFID transaction device 102 is useful where there is a concern that the transaction device information may be pirated during transmission from the device 102 to the RFID reader 104. In some instances, transaction fraud may be committed by stealing the transaction device identifier prior to the identifier being provided to an account issuer 112, thereby permitting the theft to transmit a fraudulent transaction request containing the stolen identifier. The account issuer 112 may receive the fraudulent transaction identifier and determine that the transaction device identifier is valid, which prompts the account issuer 112 to approve the transaction.

[0046] However, in accordance with the invention, the validity of

the transaction device 102 attempting to complete the transaction may be determined along with determining the validity of the transaction device identifier. This ensures that an authorized device 102 is providing the device 102 identifier information received by the account issuer 112. As noted, to facilitate the recognition of the RFID transaction device 102, the transaction device 102 may be provided an "authentication tag." The authentication tag may be, for example, a digital code or mark appended to the transaction device identifier. Alternatively, the authentication tag may be a stand alone code which is transmitted along with, but distinct from the transaction device identifier. Further still, the authentication tag may be included with, and interspersed among the transaction device identifier or any other information transmitted by the transaction device 102 to RFID reader 104.

[0047] In one exemplary embodiment, the authentication tag may be stored in the RFID transaction device database 116. The authentication tag may be provided by the database 116 to the transaction device processor 114 when the transaction device is interrogated by the RFID reader 104.

[0048] The account issuer 112 may wish to ensure that the authentication tag has not be pirated in similar manner as

was discussed with respect to the transaction device identifier. As such, the account issuer 112 may desire a secondary means of determining authentication tag validity, which may be provided to the account issuer 112 along with the tag information. The account issuer 112 may use the secondary means to verify that the authentication tag is valid by, for example, using the secondary means to locate the corresponding verifying data stored on the account issuer 112 system, which may be used to determine the authentication tag validity.

[0049] More particularly, an exemplary embodiment of the present invention uses a random number generated by a RFID transaction device random number generator 115 (or alternatively, the random number is generated by the RFID random number generator 126). Random number generator 115, 126 produces a random number, which may be provided to the account issuer 112 for use in verifying the authentication tag. That is, the account issuer 112 may use the random number to verify that the transaction device 102 providing the device 102 and transaction device information is authorized to complete a transaction request. The account issuer 112 may receive the random number and use a suitable issuer defined algorithm to

convert the random number to validating number or case validation. The account issuer 112 may then compare the validating number to validating information stored on an issuer 112 system database. If the validating code correctly corresponds to or matches the validating information, the transaction device 102 is deemed "valid." The transaction device 102 may then be permitted to communicate with the issuer 112 to complete a transaction. Otherwise, if the validating code and validating information do not match, then the transaction device 102 is deemed "invalid" and the transaction is terminated.

[0050] It should be noted that the account issuer 112 may alternatively use the random number to verity the validity of the transaction device 102 by using the random number to locate the appropriate data stored on the account issuer 112 system for use in verifying the transaction device 102 identifier or authentication tag. For example, as previously noted, the transaction device 102 identifier and/or the authentication tag are typically encrypted prior to transmission of the identifier to the RFID reader 104. As such, the transaction device 102 identifier or authentication tag are in encrypted form when received by the account issuer 112, requiring the account issuer 112 to lo-

cate the proper corresponding decryption key to decrypt the transaction device 102 identifying and authentication tag information. The account issuer 112 may use the random number to locate the corresponding decryption key. For example, the account issuer 112 may subject the random number to an algorithm designed to convert the random number into a data, which may be used to locate the corresponding decryption key. Alternatively, the algorithm may convert the random number into a proper decryption key for use in validating. Once the corresponding decryption key is located, the account issuer 112 may use the decryption key to decrypt the encrypted transaction device 102 identifier or authentication tag and thereby locate the appropriate corresponding transaction account for completion of the transaction.

[0051] Further still, as described below, where the account issuer 112 desires to determine the validity of the RFID reader 104 forwarding the transaction device 102 information, the RFID reader 104 may include a RFID reader authentication tag and a RFID reader random number generator 126. In one exemplary embodiment, the account issuer 112 may verify the RFID reader authentication tag using the random number generated by the transaction device

random number generator 115. The account issuer 112 may verify the RFID reader 104 authentication tag in similar manner as is discussed above with respect to the verification of the transaction device 102 identifier and authentication tag. That is, the account issuer 112 may receive the random number generated by the random number generator 126 and use the RFID reader random number (or the transaction device random number) to locate the data stored on account issuer 112 system which corresponds to the RFID reader authentication tag for verifying the tag's validity. In this way, the account issuer 112 may verify that the RFID reader 104 is authorized for use in transmitting the RFID transaction device 102 information. Alternatively, the account issuer 112 may receive the random number and convert the random number to validating code which may be used to validate the reader 104 in similar manner as was discussed above with respect to the transaction device 102.

[0052] Suitable random number generators for use with the invention may be able to generate a random number or code, such as an alpha numeric code for use by the account issuer 112 to verify the authentication tag's validity. In that regard, the random number generator may be any

suitable electronic random number generator as is found in the art..

[0053] The validating code, validating information, authentication tag or random number generated by the random number generator 115, 126, may take any format as desired by the account issuer 112. For example, the random number, validating code, validating information or authentication tag may be alpha-numeric, numeric, symbolic, graphical, or the like.

[0054] A clear understanding of this exemplary embodiment including the transaction device authentication tag and random number may be had with reference to Figure 1 and Figure 2. As shown, a secure RF transaction in accordance with this embodiment may begin when the RFID transaction device 102 enters the interrogation zone of the RFID reader 104 and is interrogated (step 202). The RFID transaction device random number generator 115 may produce a transaction device random number (step 204) and the transaction device database 116 may provide a transaction device authentication tag, account issuer routing number, and encrypted transaction device identifier (step 206). The transaction device 102 information, including the device 102 encrypted identifier, the transaction device

authentication tag, and the transaction device random number, and the account issuer 112 routing number, may then be provided to the processor 114 for transmitting to the RFID reader 104 via RF transmission (step 208). The transaction device 102 may provide the information to the reader 104 in ISO standardized magnetic stripe format, wherein the information may be transmitted in Track 1 / Track 2 configuration.

[0055] The RFID reader 104 may receive the transaction device 102 information and convert the information into a POS recognizable format and provide the information to the merchant POS 106 (step 210). The POS 106 may receive the transaction device information and combine the information with information concerning the requested transaction to produce a transaction request. The transaction information may include a product or merchant location identifier, as well as the terms for satisfying the transaction (e.g., price to be paid, barter points to be traded, loyalty points to be redeemed). The POS 106 may then provide the transaction request to an acquirer 110 via a network 108 (step 212).

[0056] The acquirer 110 may, in turn, provide the transaction request to the appropriate account issuer 112 for process-

ing (step 214). The acquirer 110 may identify the appropriate account issuer 112 using the routing number provided by the transaction device 102 to locate the network address corresponding to the account issuer 112, thereby permitting the acquirer 110 to provide the transaction request to the account issuer 112 maintaining the corresponding transaction device account.

[0057] The account issuer 112 may receive the transaction request and verify whether the RF transaction device authentication tag is valid (step 216). In one exemplary embodiment validating process, the account issuer 112 may use the RFID transaction device random number to locate the corresponding verifying authentication tag to which the provided device authentication tag is compared. For example, the account issuer 112 system may include a processor (not shown) for running an algorithm designed to reconstruct a tag verifying code. The algorithm may be based on any mathematical formula which may be used to convert the random number into a verifying code, which may be used to certify that the authentication tag provided by the transaction device is valid. In one instance, the account issuer 112 may validate the device authentication tag by using the verifying code to locate corre-

sponding authentication tag verification data to which the provided device authentication tag is compared or related. The authentication tag verifying data may be any data which may be used by the account issuer 112 to validate that the transaction device authentication tag, and hence, the device 102 is authorized to complete a transaction on the system 100. In this instance, if the comparison of the provided transaction authentication tag yields a desired or expected result, the tag may be considered authentic and the transaction device 102 may be considered valid. If a desired result is not yielded, the transaction device 102 may be considered invalid.

[0058] Alternatively, the account issuer 112 may use an algorithm to reconstruct a verifying code which corresponds to the transaction device authentication tag. In this instance, the verification code may be the authentication tag itself, or may be a code which the user can correlate to the authentication tag using any verifying process as is desired. Additionally, where the authentication tag is encrypted, the verification code may be used to locate the corresponding decryption key. Alternatively, the verification code itself may be the decryption key. If decryption is successfully performed using the decryption key, the ac-

count issuer 112 may deem the transaction device 102 is "valid." Otherwise, the transaction device 102 is deemed "invalid." If the authentication tag is invalid (step 218), the account issuer sends a "Transaction Invalid" message to the POS 106, thereby preventing completion of the transaction using the identified transaction device 102 (step 220). The transaction device user may then be permitted to provide an alternate means of satisfying the transaction or the transaction may be ended (step 222).

[0059] Alternatively, the account issuer 112 may determine that the authentication tag is valid (step 218). In which case, the account issuer 112 may additionally seek to verify if the validity of encrypted transaction device 102 identifier is valid (step 224). In one exemplary embodiment, the account issuer 112 may verify the validity of the encrypted device identifier by locating a corresponding decryption key with which to decrypt the transaction device identifier. In another exemplary embodiment, the account issuer 112 may use the transaction device 102 random number to locate the appropriate decryption key. The account issuer 112 may convert the random number into a verifying code, as previously described with respect to the transaction device authentication tag. That is, the account issuer

112 may use the random number to construct a validating code which may be used to locate the appropriate decryption key to the encrypted transaction device 102 identifier. Alternatively, the validating code may itself be the decryption key. In either case, the account issuer 112 may use the decryption key to decrypt the transaction account identifier and determine if the decrypted identifier corresponds to a transaction device 102 authorized to complete transactions on the system 100. The account issuer 112 may use the data stored on the account issuer 112 system to make the determination and for authorizing the completion of a transaction.

[0060] If the encrypted transaction device identifier is invalid, the account issuer 112 may provide a "Transaction Invalid" message to the POS 106 (step 220) and the transaction device 102 user is permitted to provide an alternate means of satisfying the transaction or the transaction is ended (step 222). Contrariwise, if the account issuer 112 determines that the transaction device identifier is valid (step 224) then the account issuer 112 may provide a "Transaction Valid" message to the POS 106, and the transaction is completed in accordance with the merchant's business as usual protocol (step 228).

[0061] In another exemplary embodiment of the secure RF transmission method described herein, the authorizing agent (e.g., account issuer or acquirer) may only seek to verify whether the RFID reader 104 is authorized to receive the transaction device 102 information and provide the information to a merchant POS 106. Account issuer 112 may use a RFID authentication tag and reader random number generator for that purpose. For example, in this instance, the RFID reader 104 may include a database 124 for storing and providing a RFID reader authentication tag, and a reader random number generator 126 for producing a RFID reader random number. The account issuer 112 may receive the RFID reader authentication tag and the random number and verify the validity of the authentication tag in similar manner as is described above with respect to the validation of the transaction device authentication tag. That is, the account issuer 112 may use an algorithm to convert the reader random number to a reader verifying code which may be used to locate a reader authentication verification data to which the account issuer 112 may compare to the provided reader authentication tag. Alternatively, the verifying code may be, itself, used to verify the reader authentication tag validity. Further still, al-

though the below description discusses validating the RFID reader 104 using a reader random number, it is understood that the account issuer 112 may use a transaction device random number to validate the reader 104 or reader authentication tag.

[0062] The operation of this embodiment, including the RFID reader authentication tag and reader random number generator 126, may be understood with reference to Figure 1 and Figure 3. In similar manner as with Figure 2, the method exemplified in Figure 3 may begin with the RFID transaction device 102 entering the interrogation zone and being interrogated by RFID reader 104 (step 302). The RFID transaction device 102 may then provide transaction device information (e.g., encrypted transaction device identifier, account issuer routing number) to the RFID reader 104 (step 306).

[0063] The RFID reader 104 may then receive the transaction device information from the transaction device 102 (step 308). The reader database 124 may then provide a RFID reader authentication tag (step 310), and the RFID reader random number generator 126 may generate a reader random number (step 304). The RFID reader 104 may then convert the reader authentication tag, reader random

number, and the transaction device information into POS recognizable format and provide the formatted data to the POS 106 (step 312).

[0064] The POS 106 may then receive the formatted data from the RFID reader 104 and form a transaction request, including the RFID reader authentication tag, RFID reader random number, and the transaction device information. The POS 106 may then provide the transaction request to an acquirer 110 for determining if the transaction request may be authorized (step 314).

[0065] In this exemplary embodiment, the acquirer 110 may verify the validity of the RF reader 104, instead of the RF reader 104 being validated by the account issuer 112. For example, the acquirer 110 may use the reader random number to validate the reader authentication tag. The acquirer 110 may use an algorithm to convert the reader random number to reader verification code which may be used to locate a reader authentication verifying code on an acquirer database (not shown) (step 316). The acquirer 110 may locate the corresponding authentication verifying code and compare the authenticating code to the provided reader authentication code to determine if a match exists or other similar verifying correlation can be made (step

318). Alternatively, the verifying code may be, itself, used to verify the reader authentication tag validity.

[0066] If a correlation or match cannot be made with the RFID reader authentication tag (step 322), then the RFID reader 104 is considered invalid for use in conducting a transaction on the system 100, and the acquirer 110 forwards a "Transaction Invalid" message to the POS 106 (step 326). Alternatively, if a correlation or match is made (step 322), the RFID reader 104 is considered valid, and the acquirer 110 forwards the transaction request to an account issuer 112 for validation of the transaction device 102 identifier (step 323) by, for example, locating the proper decryption key. The account issuer 112 may then decrypt the transaction device identifier for validation.

[0067] If the transaction device identifier is deemed invalid (step 324), then the account issuer 112 may provide a "Transaction Invalid" message to the POS 106 (step 326), and the device 102 user may be permitted to provide alternate means of satisfying the transaction, or the transaction may be ended (step 328). Otherwise, the account issuer 112 may validate the transaction device 102 (step 324) and send a "Transaction Valid" message to the POS 106 (step 330) and the transaction is completed under busi-

ness as usual standards.

[0068] In yet another exemplary embodiment of the invention, an account issuer 112 may desire to determine whether both the RFID transaction device 102 and the RFID reader 104 are valid for use in completing a transaction on the secure RF transmission system 100. In this instance, both RFID transaction device 102, and RFID reader 104 include a random number generator 115 and 126, respectively. In addition, RFID transaction device database 116 may provide a transaction device authentication tag and RFID reader database 124 may provide a reader authentication tag. As such, an acquirer 110 and/or an account issuer 112 may use the random numbers and the authentication tags to verify the validity of the transaction device 102 and the reader 104 using any validating method as described above.

[0069] With reference to Figure 4 and continued reference to Figure 1, the operation of the secure RF transmission system including a reader random number and a transaction device random number may be understood. The operation of this method may begin in similar manner as with the method described with respect to steps 302-310 in FIGURE That is, the transaction device 102 may enter an in-

terrogation zone and be interrogated by the RFID reader 104 (step 402); the transaction device random number generator 115 may generate a transaction device random number and provide the device random number to the device processor 114 (step 404); the transaction device database 116 may provide a routing number, transaction device authentication tag and encrypted transaction device identifier to the processor 114 (step 406); and the processor 114 may provide the transaction device information, including the routing number, RFID transaction device authentication tag, encrypted transaction account identifier, transaction device random number, and transaction device counter total transactions counted value, to the RFID reader 104 via RF transmission (step 408).

[0070] Once the RFID reader receives the transaction device information, the RFID reader database 124 provides a RFID reader authentication tag to the RFID reader processor 122 (step 412). In addition, the RFID reader random number generator produces a reader random number and provides the reader random number to the RFID reader processor 122 (step 410). The RFID reader 104 then converts the transaction device information and the RFID reader random number and authentication tag in a POS

readable format and provides the converted information to the POS 106 (step 416). The POS 106 may then forward the converted information and any transaction request information to an authorizing agent for validation.

[0071] In one exemplary embodiment, the validity of the RFID reader 104 may be verified at the acquirer 110 location in similar manner as was described with respect to FIGURE Alternatively, the present exemplary embodiment describes the RFID reader 104 being validated by the account issuer 112, only by way of illustration.

[0072] In accordance with the embodiment illustrated, the POS 106 may provide the converted information to an acquirer 110 (step 418) and the acquirer 110 may provide the converted information to an account issuer 112 for validation (step 420). In this manner, the account issuer 112 may validate the RFID transaction device authentication tag and the RFID reader authentication tag in similar manner as was described with respect to step 220 of Figure 2 and step 322 of Figure 3 (steps 426 and 428, respectively).

[0073] If the account issuer 112 determines that the RFID device authentication tag or the RFID reader authentication tag are invalid, then the account issuer 112 may provide the POS 106 with a "Transaction Invalid" message, thereby

preventing the transaction from being completed (step 430). The transaction device 102 user may then be permitted to provide alternate means for satisfying the transaction, or the transaction may be terminated (step 432). Alternatively, if the transaction device authentication tag and the reader authentication tag are valid, then the account issuer 112 may further seek to determine whether the information provided by transaction device 102 is valid. For example, the account issuer 112 may seek to validate the encrypted transaction device identifier using any method described above (step 434).

[0074] Once the RFID transaction device authentication tag, the RFID reader authentication tag and the transaction device identifier are validated the account issuer 112 may provide a "Transaction Valid" message to the POS 106, and the merchant may seek satisfaction of the transaction request under the merchant's business as usual standards.

[0075] In accordance with the various embodiments described, the present invention addresses the problem of securing a RF transaction completed by a RFID transaction device. The invention provides a system and method for an account issuer to determine if the RFID transaction device and/or the RFID reader is a valid device for completing a

transaction on a RF transaction system. The account issuer can determine whether the reader or transaction device is valid by verifying the reader or device authentication tag and/or encryption code. Similarly, the account issuer may determine the validity of the reader by validating the reader authentication code. It should be noted, however, that the present invention contemplates various arrangements wherein the reader and/or the transaction device may be validated. In addition, the reader and the transaction device may be validated in the same validating process, and each or both may be validated by the acquirer or the account issuer, as desired. In addition, validation of the reader may take place in real-time or under some proscribed ordering.

[0076] The preceding detailed description of exemplary embodiments of the invention makes reference to the accompanying drawings, which show the exemplary embodiment by way of illustration. While these exemplary embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the invention. For

example, the RFID reader may include an RFID reader encrypted identifier stored in the reader database, which may be validated by the account issuer in similar manner as with the transaction device encrypted identifier. In addition, the steps recited in any of the method or process claims may be executed in any order and are not limited to the order presented or method steps may be added or eliminated as desired. For example, in a particularly exemplary embodiment of the invention the reader may not include an authentication tag, eliminating the need for a step providing a reader authentication tag. Also, the reader may be provided with an encrypted reader identifier, in which case, method steps may be added for verifying the reader identifier. Further, the present invention may be practiced using one or more servers, as necessary. Thus, the preceding detailed description is presented for purposes of illustration only and not of limitation, and the scope of the invention is defined by the preceding description, and with respect to the attached claims.